The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

A. JOSEPH DeNUCCI
AUDITOR

NO. 2002-0197-4C

INDEPENDENT STATE AUDITOR'S REPORT ON INFORMATION TECHNOLOGY-RELATED CONTROLS AT MASSASOIT COMMUNITY COLLEGE

July 1, 2001 to January 30, 2002

OFFICIAL AUDIT REPORT

APRIL 16, 2002

2002-0197-4C

TABLE OF CONTENTS

INTRODUCTION

Massasoit Community College (MCC) is a two-year, public college that provides affordable, higher education primarily to residents of the City of Brockton and surrounding communities. MCC, which is authorized under Massachusetts General Laws Chapter 15A, Section 5, held its first classes beginning in September 1966. The College is governed by the Commonwealth's Board of Higher Education and is overseen by a twelve-member board of trustees appointed by the Governor. The College, which has approximately 4,400 day students and 2,400 evening students, is an educational institution designed to provide post-secondary educational opportunities to men and women of diverse backgrounds and goals. MCC awards associate degrees and/or certificates to students who complete prescribed courses of study.

The College's administrative and academic mission and operations are supported by information technology services provided by the Office of Information Technology (OIT). OIT is comprised of 15 full-time staff members, including a Chief Information Officer who reports to the Vice President of Administration and Finance. The OIT operates both the administrative and academic data centers, as well as media services.

The College currently operates two primary application systems in parallel, the APECS (Advanced Programs for Educational Solutions) and the BANNER system. At the time of our audit, the APECS application served as the College's primary financial management, administrative, admissions, registration, financial aid, student receivables, billing, and work-study payroll systems, and the BANNER application was used to process certain accounts receivable functions. The College plans to migrate fully to the BANNER system by April 2003. The APECS application resides on a Unisys NX 4601 mainframe computer which utilizes an MCP operating system. The BANNER application resides on five file servers (four Sun Microsystems and one Dell) that operate using the database file server.

Local Area Networks (LANs) are used to support administrative and academic functions. The administrative LAN is comprised of approximately 280 microcomputers that can access the mainframe and the file servers connected to the LAN. MCC's academic LAN is supported by seven Novell authentification, file and print servers. The Novell servers, which utilize version 4.11 Netware, support twelve of the fifteen academic classrooms and computer labs comprising 550 microcomputers. In addition, 189 stand-alone microcomputers were assigned to faculty and academic support staff members.

The Office of the State Auditor's examination focused on a review of certain information technology-related general controls over the MCC's computer operations.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an information technology (IT)-related audit at Massasoit Community College from August 9, 2001 to January 30, 2002. The audit covered the period of July 1, 2001 to January 30, 2002.

The scope of our IT audit included an evaluation of IT-related general controls for the administrative and academic IT functions. Areas reviewed included IT-related organization and management, physical security, environmental protection, logical access security, on-site and off-site storage of magnetic backup media, and disaster recovery and business continuity planning. We also examined controls over IT-related service contracts and procurement and inventory record-keeping of IT-related assets.

Audit Objectives

Our primary audit objective regarding the examination of IT-related controls was to determine whether the College's administrative and academic IT environment was sufficiently controlled to support its automated systems and to safeguard IT-related assets. We sought to determine whether the IT-related internal control environment, including policies, procedures, and organizational and management structure provided reasonable assurance that IT-related objectives would be achieved to support the College's business objectives and to prevent and detect undesired events. Our audit objective regarding organization and management was to determine whether IT-related roles and responsibilities were clearly defined, appropriate organizational controls were in place, and that IT-related policies and procedures adequately addressed the areas under our review. We sought to determine whether MCC had implemented written and approved policies and procedures regarding authorized access, the safeguarding of assets, IT-related contract management, business continuity planning, and the proper accounting of IT-related assets.

We sought to determine whether adequate physical security and environmental protection were in place over and within areas housing IT-related assets to provide reasonable assurance that access would be available to only authorized users and that damage to, or loss of, computer equipment, software, and data files would be prevented or detected. The areas reviewed were the College's administrative and academic data centers, administrative offices, computer laboratories and the administrative and academic off-site backup media storage location. Also with respect to access security, a further objective was to determine whether adequate controls were in place to

prevent and detect unauthorized logical access to MCC's systems. We determined whether staff monitored and notified IT management of users who no longer required access, or needed to have their access privileges changed, due to employment termination and change in their job-related responsibilities.

We sought to determine whether an adequate disaster recovery and business continuity plan was in place to provide reasonable assurance that computer functions would be able to regain processing and operations within an acceptable period should a disaster render computerized functions inoperable or inaccessible. In addition, we determined whether adequate on-site and off-site storage was being provided for backup copies of mission-critical and essential application software, data files, and archival copies of data files.

Our objective regarding the proper accounting of IT-related assets was to determine whether there were adequate controls in place provided reasonable assurance that all IT-related equipment, including computer equipment and software, were properly recorded in the College's inventory record, and were properly accounted for and reported to the Office of the State Comptroller in accordance with laws and regulations. A further objective was to evaluate whether adequate controls were in place over IT-related outsourced service contracts and whether all vendors doing business with the College were properly registered with the Corporations Division within the Massachusetts Office of Secretary of State and whether services and deliverables were being provided to the College in accordance with the contracts.

Audit Methodology

To determine audit scope and objectives, we conducted pre-audit work, which included obtaining and recording an understanding of relevant IT operations, reviewing and evaluating internal controls, and interviewing senior management to discuss the College's control environment. In conjunction with our review of the internal control environment, we determined whether MCC had developed, reviewed, approved, and implemented, internal control documentation, including IT-related policies and procedures. In order to obtain a preliminary understanding of the College's IT-related contract administration and the safeguarding of, accounting for, and reporting on property and equipment, we interviewed College management and staff, reviewed relevant Commonwealth statutes and regulations regarding fixed-asset management, and reviewed the College's related policies and procedures, selected contracts, and records.

Regarding our examination of organization and management, we interviewed senior management; obtained, reviewed, and analyzed existing IT-related policies, standards,

procedures, and the IT strategic plan to determine their adequacy and assessed IT-related management practices. To determine whether an IT-related steering committee was in place and operating to help provide adequate oversight of IT functions and processes across the College, we interviewed senior management, IT staff, and reviewed minutes of steering committee meetings. To determine whether MCC's IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities and technical knowledge requirements, we obtained a current list of the personnel employed by the Office of Information Technology and a copy of IT-related job descriptions and job specifications and reviewed and compared the job descriptions and job specifications to current IT-related assignments and responsibilities.

To evaluate physical security, we interviewed senior management and security personnel, conducted walk-throughs and reviewed security violations and/or incidents. We also obtained a list of employees who had keys to the College's data centers and through observation, determined the adequacy of physical security controls for data center access, such as locks, physical access procedures, visitor logs, motion detectors, and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were employees of the College. Further, to determine the adequacy of physical security controls regarding microcomputer systems located throughout the College, we conducted site visits to office areas, computer labs, and on-site and off-site storage areas.

To determine whether IT resources were subject to adequate environmental protection, we conducted site visits to areas housing IT equipment and backup copies of software and data files. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supplies, emergency lighting, and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and documentation reviews. To determine the adequacy of environmental controls, we conducted a walk-through and evaluated controls in place within the data centers and selected areas and assessed the sufficiency of control-related policies and procedures.

To determine whether MCC could account for all copies of application software residing on its stand-alone and networked workstations, we determined whether a software inventory record was available, evaluated control procedures, and interviewed MCC management. In the absence of a software inventory record, to identify the nature and extent of software, we requested a list of software installed on MCC's systems and reviewed related documentation such as purchase orders and licenses for application software residing on the minicomputer and microcomputer systems. To determine whether appropriate controls were in place to prevent and detect the use

of unauthorized software, we reviewed policies and procedures and interviewed IT management and staff.

Our tests of system access security included a review of access privileges for those staff members who were authorized to access the minicomputers and the client/server systems. We determined whether logon ID and password access was established for authorized users and employees of the College. We determined the frequency with which all staff authorized to access the automated system were required to change their passwords. We compared the list of staff authorized to access the information systems with the current MCC employee list to determine whether individuals having access to the systems were current employees. We also reviewed password administration controls, such as granting passwords, required length and composition of passwords, related security procedures, frequency of password changes and restrictions on using previously used passwords.

To assess the adequacy of business continuity planning, we reviewed disaster recovery and business continuity planning procedures documented by the College for the administrative data center. We interviewed MCC management to determine whether the criticality of application systems had been assessed and whether risks and exposures to the computer operations had been evaluated. We also reviewed the current status of formal business continuity planning. Further, we reviewed the adequacy of provisions for on-site and off-site storage of critical backup media and conducted site visits to the administrative computing storage areas to assess the adequacy of physical security and environmental protection. We assessed the adequacy of inventory control procedures for backup copies of magnetic media.

To accomplish our review of IT-related contracts and services for fiscal year 2001 and the first six months of fiscal year 2002, we examined contract-related policies and procedures. In addition, we interviewed management and obtained and reviewed copies of selected contracts to determine whether they were approved by appropriate parties and whether the proper signatures and dates were included in accordance with state requirements. We determined whether desired deliverables and services were provided and whether vendors that were incorporated within, or outside of Massachusetts, were properly registered with the Commonwealth's Office of the Secretary of State.

To determine whether adequate controls were in place and in effect to properly account for the College's IT-related property and equipment, we reviewed inventory control procedures for hardware and software. We determined whether computer equipment was properly tagged with state identification numbers and serial numbers and whether the serial numbers attached to the equipment were properly recorded on the hardware inventory list. To determine whether the

records for hardware for fiscal year 2001 were current, accurate, complete, and valid, we chose for testing a judgmental sample of 59 out of 2,199 items of MCC's computer equipment. We traced the state identification numbers of the hardware items listed on the inventory record to the actual equipment on hand. We judgmentally selected an additional ten (10) items of computer equipment and traced the items to the inventory record. We confirmed purchase documentation for ten (10) hardware items purchased during the first quarter of fiscal year 2002, valued at $49,596 to the inventory record and then to the equipment on hand.

We determined whether MCC had complied with the annual GAAP reporting requirements, as promulgated by the Commonwealth's Office of the State Comptroller, by submitting accurate, complete, and valid fixed-asset information and supporting financial documentation in a timely manner.

The audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and industry auditing standards.

AUDIT SUMMARY

Based on the results of our audit, internal controls in place at Massasoit Community College provided reasonable assurance that control objectives related to organization and management, and physical security and environmental protection over IT resources would be met. Specifically, we found that adequate physical and environmental protection controls were in place for the College's data processing environment, including office areas, the data center, and computer labs. In addition, we determined that procedures regarding the generation of on-site and off-site storage of backup copies of magnetic media were adequate. However, our audit revealed that controls needed to be implemented or strengthened in the areas of IT-related hardware and software inventory, logical access security, and disaster recovery and business continuity planning.

We found that controls related to IT organization and management provided reasonable assurance that certain IT management control objectives would be met. Our audit disclosed that the College had a well-defined IT organizational structure that provided for communication and oversight of the academic and administrative IT functions. The organizational structure provided for an established chain of command, an acceptable span of management, and clear points of accountability. IT management and staff were well aware of their responsibilities, and IT-related job descriptions and job specifications had been developed or updated to reflect current assignments, technical knowledge, and skill requirements. Our review of IT-related planning found that the College had developed an overall strategic plan for 2001 through 2004, dated August 1, 2001, but as of the time of our audit, the plan had not been fully approved by the College's Board of Trustees. We encourage the College to proceed with plans to strengthen and formalize an IT planning process that will yield strategic and tactical IT plans to support the College's mission.

Our examination of physical security and environmental protection found that controls provided reasonable assurance that control objectives related to authorized physical access, general housekeeping; restricted use of electrical appliances; air conditioning and humidity control; fire prevention, detection, and suppression; emergency lighting and power shutoff would be met for the administrative and academic data centers. In addition, we found that appropriate physical security and environmental protection controls were in place for the business office, computer labs, and for the on-site and off-site storage location of computer media.

Our review of logical access security for the APECS (Advanced Programs for Educational Solutions) and BANNER Systems that supports administrative operations indicated that access security administration needed to be strengthened. We found that although procedures were in

place to authorize and activate access privileges and to periodically change passwords, procedures needed to be strengthened to ensure timely deactivation of access privileges no longer authorized or needed. We found that the security administrator was not consistently being notified in a timely manner of changes in employment status of users having access to automated systems by department heads or the Human Resources Department. Our tests of authorized users to the APECS and BANNER systems revealed that at the time of our test, 28 (4.8%), out of 583 user accounts were active for individuals no longer employed by the College. We recommend that the College require department heads, deans, and the Human Resources Department to promptly notify the security administrator of changes in employee status that could warrant changes of access levels or complete deactivation of user access privileges.

Our examination of inventory control revealed that the College had maintained two separate inventory records, one to account for property and equipment and the other for information technology-related equipment. In addition, the College had documented policies and procedures regarding inventory control. Based on our examination, we found that increased effort was needed to ensure that hardware and software are properly accounted for. Audit test results drawn from a judgmental sample of IT-related items, indicated that not all items were tagged and that there were a number of instances where the location of the items as designated on the inventory record was incorrect. Based upon a sample of 79 physically-located items, three were not properly tagged, three had the wrong location indicated on the inventory record, and four were not recorded on the master inventory record of IT-related equipment. In addition, the inventory record did not provide unit values or acquisition dates. We recommend that the College consider using the BANNER inventory module to support inventory and configuration management and IT infrastructure planning requirements.

Regarding software, we found that adequate controls were not in place to ensure that software products residing on microcomputers were properly accounted for or that unauthorized use or copying of software would be prevented or detected. Establishment of a software inventory record for the academic and administrative IT departments would provide a base of comparison for periodic checks of installed software to determine whether only authorized software was installed. The College should consider using LAN-based software to identify the software packages installed on file servers and networked workstations.

Although we determined that procedures regarding the generation of backup copies of magnetic media and the storage of the backup media at secure on-site and off-site locations were adequate, our review indicated that the level of disaster recovery and business continuity planning needed to be strengthened. We found that there was a general absence of documented plans to

address disaster recovery and business continuity for automated operations. Our audit disclosed that the College did not have a formal disaster recovery and business continuity plan to provide reasonable assurance that mission-critical and essential data processing operations for administrative and academic functions could be regained effectively and in a timely manner, should a disaster render automated systems inoperable. Although we found that the College had begun to formulate a business continuity strategy, an alternate site contingency plan had not yet been developed, nor had user area plans been established to document the procedures required to regain business operations in the event of a disaster.

Our review of the College's IT-related service contracts revealed that all contracts were properly signed and approved and that services had been delivered. In addition, all vendors incorporated as either a foreign or domestic corporation were found to be properly registered with the Commonwealth's Office of the Secretary of State.

AUDIT RESULTS

1. Hardware and Software Inventory

Our review of hardware and software inventory revealed that controls needed to be strengthened to provide for the proper accounting of these assets. We found that the MCC's Office of Information Technology was responsible for maintaining the College's computer hardware and software inventory records. At the time of our audit the College could not provide a current and complete record for all IT-related items. We also determined that a physical inventory had not been performed since July 1999 to assist in verifying the inventory record.

Our inventory tests conducted against the inventory record provided by OIT during the course of the audit, revealed that not all identified locations were correct and that some items of equipment did not have proper inventory tag numbers attached. Our examination of fixed asset inventory control disclosed that three (4%) out of 79 IT-related items within our judgmental sample could not be readily located from the master inventory record, but were subsequently found at a location other than the one indicated on the system of record. Further, an additional three (4%) items out of 79 items of computer equipment tested were found not to be properly tagged with MCC identification numbers as required by the Office of State Comptroller. In addition, our audit tests revealed that four of the 79 physically-located items in our sample were not recorded on the inventory record for IT-related equipment. A review of the inventory record indicated that there were no unit values and acquisition dates associated for any of the items on the list. A test performed on IT-related purchases from the first quarter of fiscal year 2002, with a total value of $49,596, confirmed that all ten items of equipment purchased were correctly listed on the inventory record.

At the time of our review of software inventory controls, management could not provide a software inventory record. Because of the lack of an up-to-date, accurate, and complete record of software inventory, the College could neither account for all copies of software installed on the LAN and microcomputers, nor determine whether only authorized software was residing on their systems. In addition, the absence of a software inventory record precluded an accounting of the total number of software copies allowed per the various software license agreements.

Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained for all computer equipment and software and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record. In addition, prudent business practices advocate that the software inventory

record be used to help prevent unnecessary software expenditures and to detect theft, unauthorized installation of software, and potential software copyright infringements.

Reconciliation of software inventory records to software residing on computers would provide a detective control to identify misplaced, lost, stolen, unauthorized, or potentially illegal copies of software. Asset control is facilitated when all software is properly identified, indicating the computer on which it resides.

The College's "Internal Control Plan" dated September 26, 2001 states that "the College is required to properly account for all fixed-asset transactions, including the proper recording and the reconciliation of a periodic inventory of all fixed assets. This physical reconciliation should be completed as of June 30th of each fiscal year."

Complete and accurate inventory records of state-owned assets are required by law. In accordance with MGL, Chapter 7, Subsection 4A, each state agency is required to record and report state-owned assets to control agencies, such as the Office of the State Comptroller (OSC). Our audit confirmed that the College had submitted a GAAP report indicating total values for hardware and software.

Generally accepted industry standards and sound management practices indicate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of l989, states, in part, that " . . . the agency shall be responsible for maintaining accountability for the custody and use of resources and [shall] assign qualified individuals for that purpose, and [that] periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts."

Shortcomings in inventory control were the result of lack of management attention and proper assignment of asset control responsibilities. The absence of an accurate inventory record for software may hinder the College's ability to determine whether unauthorized and/or illegal software has been installed on microcomputers. Undetected copyright infringements regarding potentially illegal software copies could place the College at risk of possible legal action. The absence of proper identification number tagging may hinder the College from detecting lost or stolen assets.

Recommendation:

The College should enhance controls over its record-keeping to provide for maintenance of a perpetual hardware and software inventory record. Specifically, we recommend that the College adhere to the policies and procedures outlined in the MCC's "Internal Control Plan" to ensure that a perpetual hardware and software inventory record be maintained and periodically verified

through reconciliation to physical hardware and the software residing on computer equipment. We recommend control procedures be implemented to ensure that the inventory records are maintained in an accurate, complete, and timely manner. The inventory record should reflect any changes to computer hardware and software packages installed or available for installation. Hardware and software inventory records should include pertinent information, such as the name of the software product, acquisition source, cost, serial and model numbers, version number, number of copies of software acquired and allowed, and the location of the computer on which original versions and copies reside. We recommend that MCC management review all of their property and equipment for proper identification tagging. We recommend that the College consider using the BANNER inventory module to support inventory and configuration management requirements.

Auditee's Response:

The College acknowledges that the current, manual methods of documenting hardware and software inventory are inadequate to meet the need and complexity of its information technology environment. During the past year and with the assistance of our Collegis partner, we have completed analysis and planning that will result in an infrastructure that is capable of building an automated process for inventory. Further, the Office of Information Technology (OIT) contributed its policies and procedures section to the College's "Internal Control Plan." OIT will adhere to those provisions.

The first step toward development of an automated inventory system required the upgrading of our campus-wide network to a high-speed "backbone' of connections to all computers and network attached devices. The upgrades were installed in August of 2001. This new "gigabit" speed "backbone" will allow sufficient bandwidth for traffic on both campuses to maintain daily work activity and provide the College with run management software that can automate asset tracking for computer equipment and software.

Second, a policy of "life-cycle" replacement has been put in place to remove out-dated technology that has very limited capacity for automated asset tracking. Replacement computers and peripherals can be scanned for a host of asset requirements including identification of machine type, model, serial, motherboard, processor, network connection, date of installation, and other features. Fiscal Year 2002-2003 will be the second year of our four-year life cycle replacement plan.

Third, the current hardware inventory was completed in July and August of 2001. Manual entry of the data, analysis of missing tags, incorrect labeling, and changes of location are still being processed. To eliminate this prolonged cycle, the College has evaluated software that will be able to use the network to pull hardware information from every connected machine. A decision to purchase the software will be made no later than April 15, 2002. Full implementation of the chosen product will allow the College to have a baseline for a "perpetual hardware and software inventory" completed prior to the beginning of the 2002-2003 fiscal year. Information on new purchases is being captured on the new "Banner" system. These data will provide an initial input of new equipment to

the asset tracking software at the time of arrival on campus. The identification of new arrivals will be a primary step toward insuring proper tagging, purchase and installation date, cost information, and initial configuration that will drive the "perpetual" record.
.

Auditor's Reply:

We are pleased that the College is taking steps to strengthen the integrity of the fixed-asset inventory record. The implementation of the BANNER inventory module should aid the College in maintaining a perpetual inventory record. We will examine the progress made to the fixed-asset inventory record during our follow-up audit.

2. Logical Access Security

Our audit revealed that system access security over MCC's local area network needed to be strengthened to ensure that only authorized users have access to the system. We found that, although there were written policies and procedures in place to for the proper authorization and activation of system users, there were no written IT policies and procedures in place when an individual terminated employment at the College, and no written notification was being given from the College's Human Resources Department, department heads, or deans of changes in employee status (e.g., terminations, leaves of absences, or transfers). In addition, adequate procedures were not in place for administering passwords and monitoring system access. Our tests of access security for the LAN indicated that, contrary to sound access-security practices, there were active user IDs and passwords for individuals who were no longer employed by the College.

We found that there were written policies and procedures in place requiring that the Office of Information Technology be informed when an employee terminates employment at the College. However, written notification was not consistently being given from the College's Human Resources Department, department heads, or deans informing the Office of Information Technology of changes in employee status (e.g., terminations, leaves of absences, or transfers) that would necessitate deactivation of user accounts. Our tests of access security for the administrative LAN indicated that, contrary to sound access-security practices, sufficient documentary evidence was not available to indicate timely notification to the Office of Information Technology and subsequent deactivation of user accounts. Our tests disclosed that there were active user IDs and passwords for three individuals who were no longer employed by

the College. Our tests of the APECS and BANNER systems indicated that 28 (4.8%), out of 583 users were not listed on the official employee record.

Our audit disclosed that the College could neither t provide information as to the last date of use of user access accounts for the former employees still having active user privileges, nor provide documentation as to dates that these users had terminated their employment. Our audit disclosed that although MCC's Computer Use Policy documented security controls for logical access security to the LAN and microcomputers, the policy did not suffiently document the security controls for password deactivation procedures. The failure to deactivate user accounts in a timely manner places the College at risk to unauthorized use of established privileges (using another individual's user account having higher access privileges) or to unauthorized access.

Access to computer systems, program applications, and data files should be authorized on a need-to-know and need-to-perform basis. In addition, considerations of need-to-protect should be applied to data elements when security requirements are being established. To ensure that only authorized access privileges are maintained, timely notification should be made to the security administrator of any changes in user status that would impact their level of authorization. For example, Human Resources should notify the security administrator of changes in employment status so that access privileges may be deactivated in a timely manner for individuals no longer needing access. Our review indicated that there was evidence of initial authorization, but that procedures were not in place to inform the security administration of changes in employment status. As a result, critical information on the College's systems may have been vulnerable to unauthorized access, alterations, and deletions.

The Commonwealth of Massachusetts' "Internal Control Guide for Departments' promulgated by the Office of the State Comptroller states in part…"an employee's password should be changed or deleted immediately upon notice of his/her termination, transfer, or change in responsibity." In addition, computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for proper protection of information assets. The policies and procedures should address authorization for system users, development of user IDs and passwords, authentication of users, establishment of audit trails, notification of changes in user status, frequency of password changes, and procedures to be followed in the event of an unauthorized access attempt or unauthorized access. The policies and procedures should also address emergency access guidelines for critical applications to ensure that under emergency or disaster recovery situations, only authorized access is granted.

Formal policies and procedures for system access security should be in place that address password administration, activation and deactivation of access privileges, and monitoring of

system access. The failure to develop written system access security policies and procedures and implement adequate controls places critical user files at risk to unauthorized access, modification, or loss.

Recommendation:

We recommend that procedures be established requiring written notification from the College's Human Resources Department and department heads of changes in personnel status (leaves of absence, changes in responsibilities, and terminations of employment) to the security administrator to help ensure timely modification or deactivation of access privileges. We recommend that the security administrator review, on a periodic or cyclical basis, with department heads individuals authorized to access automated systems and verify that their access privileges are appropriate to their job responsibilities.

Auditee's Response:

The College acknowledges that its current methods of ensuring logical access security are inadequate. Policy review and re-writing are in progress to eliminate the gaps in the determination of active, inactive, and "to be" removed status of users on the College's network systems. OIT is working with the newly appointed Director of Human Resources to establish a written document and set of procedures that will inform both departments of any change in job requirements, transfers, active/inactive status, or termination of employees. Recommendations for the timeliness of this process and responsibility of managers to communicate the required information will be mandated and supervisors will be trained. This process will be completed by June 30, 2002.

OIT is presently working on developing a strategy to log access security for all administrative networked systems. Additionally, planning for implementing access security for the "Banner" system is being developed and implemented during our current system conversion. The present system of decentralized servers has been an obstacle to a unified system. However, as the network infrastructure and server consolidation phases of our IT Strategic Plan, which was adopted by the Board of Trustees in August 2001, are implemented, access security will become more structured, capable of producing audit trails, and in compliance with Commonwealth guidelines.

Auditor's Reply:

We are pleased that the College's OIT Department has begun working with the Human Resources Department in establishing written policies and procedures to inform one another of any change in job requirements, transfers, active/inactive status, or termination of employees. We are pleased that the College intends to implement its IT Strategic Plan, which calls for a more structured access security policy. We will examine the College's efforts to strengthen logical access security during our follow-up audit.

3. Disaster Recovery and Business Continuity Planning

MCC did not have a formal disaster recovery and business continuity plan to provide reasonable assurance that critical data processing operations for administrative and academic functions could be regained effectively and in a timely manner, should a disaster render automated systems inoperable. Although backup copies of critical and essential software and data were being made, specific arrangements had not been made to provide for alternate-site processing. In this regard, we found that there was no agreement in place with another organization for alternate-site processing should the LAN be unusable or inaccessible. Further, the College had not assessed the relative criticality of their automated systems to determine the extent of potential risks and exposure to data processing operations. Our audit also revealed that system users had not developed user-area contingency plans to address a potential loss of their automated processing.

Without adequate disaster recovery and contingency planning, including required user-area plans, the College was at risk of severely degraded or failed processing should automated capabilities be disrupted or lost. A loss of processing capabilities could adversely affect all administrative and academic functions supported by the data centers. Depending on when a disaster occurred during the academic year, the impact could hamper the College's ability to function. Furthermore, the absence of a comprehensive and tested disaster recovery plan could result in unnecessary costs, significant processing delays and loss of good will by students and faculty.

Disaster recovery and business continuity plans should be well tested to reduce time and the risk of errors and omissions when restoring computer operations. An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the data processing facility and, accordingly, the manner and order in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate-processing site. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Sound management practices, as well as industry and government standards, advocate the need for a comprehensive and effective backup and disaster recovery and business continuity

plan. Contingency planning should be viewed as a process to be incorporated with the functions of the organization, rather than as a project with successful completion upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that would identify a change in criticality and amend the contingency plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact to existing disaster recovery and contingency plans.

Recommendation:

The College should assess the criticality of automated systems to identify application priorities and critical resources. An analysis should be conducted to identify risks and exposures relating to the College's data processing operations and microcomputer environment. The College should identify potential processing alternatives and resources to be utilized should a disaster disrupt its data processing or business operations. Based upon these results, and input solicited from management and user departments, a written disaster recovery and business continuity plan should be developed, reviewed, and tested, to the extent possible; approved by senior management; and implemented.

We further recommend that procedures be developed to ensure that the criticality of systems is periodically reassessed, that the impact of changes in user needs or automated systems is evaluated, and that staff are adequately trained in executing recovery plans. Upon a major change to systems or equipment, or at least annually, the disaster recovery plan should be reviewed, updated, and tested to ensure that it is current, accurate, and complete. The business continuity plan, or specific sections of it, should be distributed to appropriate personnel, and a complete copy of the plan should be stored in a secure off-site location.

Auditee's Response:

> *Current administrative systems have been undergoing risk analysis and administrative system evaluation of criticality based upon analyses completed by Collegis consultants and OIT staff. Draft policies and procedures were presented to the Board of Trustees for their information in February 2002. This process will be completed in May, documented to Senior Management by June 1, 2002 and presented to the Board for adoption that month. The College will follow this adoption with training of staff to ensure that they are adequately prepared to execute recovery plans.*
>
> *The recently developed policy on disaster recovery and business resumption planning outlines a set of rigorous processes for annual analysis, review, and notification of the status of recovery and resumption plans. Copies of the plan have been disseminated to off-site locations for security, and the processes of training, cross training, and testing procedures has begun. The College currently is engaged in discussions with Bristol*

Community College to map plans that will provide an off-site processing environment in the event of a disaster involving the loss of our data center.

Auditor's Reply:

We are pleased that the College acknowledges the need to assess the criticality of automated systems and will be taking steps toward developing a business continuity strategy for the College. We encourage the College to develop a comprehensive business continuity plan for all required administrative and academic applications. We strongly recommend user department participation in the development and testing of business continuity plans as well as that of the Office of Information Technology. Since business continuity planning requires that recovery and contingency plans be maintained, we recommend that responsibilities for maintaining the plans be assigned and that appropriate change control procedures be implemented to ensure that viable, authorized plans are in effect.